(19) JAPANESE PATENT OFFICE (JP)

(12) KOKAI TOKUHYO PATENT GAZETTE (A)

(11) PATENT APPLICATION PUBLICATION NO. 2002-290396

(43) Publication Date: October 4, 2002

(51) Int. Cl.[7]:	Identification Codes:	FI			Theme Codes (Reference):
H 04 L 9/16		H 04 L	9/00	643	5J104
9/08				601E	

Examination Request: Not filed

No. of Claims: 10 (Total of 9 pages; OL)

(21) Filing No.: 2001-85823

(22) Filing Date: March 23, 2001

(71) Applicant: 000003078
Toshiba Corporation
1-1 Shibaura, Minato-ku
Tokyo

(72) Inventor: Noboru Suzuki
Toshiba Corporation, Ome Complex
2-9 Suehiro-cho, Ome-shi
Tokyo

(74) Agent: 100058479
Takahisa Suzue, Patent Attorney,
and 6 others

F Terms (Reference):
5J104 AA01 AA16 AA34 EA04 EA24
JA03 NA02 PA07

(54) Title: ENCRYPTION KEY UPDATE SYSTEM AND ENCRYPTION KEY UPDATE METHOD

(57) Abstract

Problem

[To provide] an encryption key update system that enables the encryption keys for all devices that are transmitting and receiving data to be updated synchronously without requiring complicated operations such as the setting and input of an encryption key on the part of the user.

Means to solve

With this encryption key update system, an encryption key list on which are recorded multiple encryption keys is distributed in advance to all of the devices that perform data encryption with a common encryption key method. Furthermore, a program that selects one or more encryption keys from this encryption key list based on a prescribed rule also is distributed to each device. Then, for example, for a given period, each device selects 'common encryption key 1' as the encryption key, and automatically sets that key in the communication environment. Subsequently, with a given date and time as the boundary, each device discards that 'common encryption key 1' and selects 'common encryption key 2' as the encryption key, which it automatically sets in the communication environment.

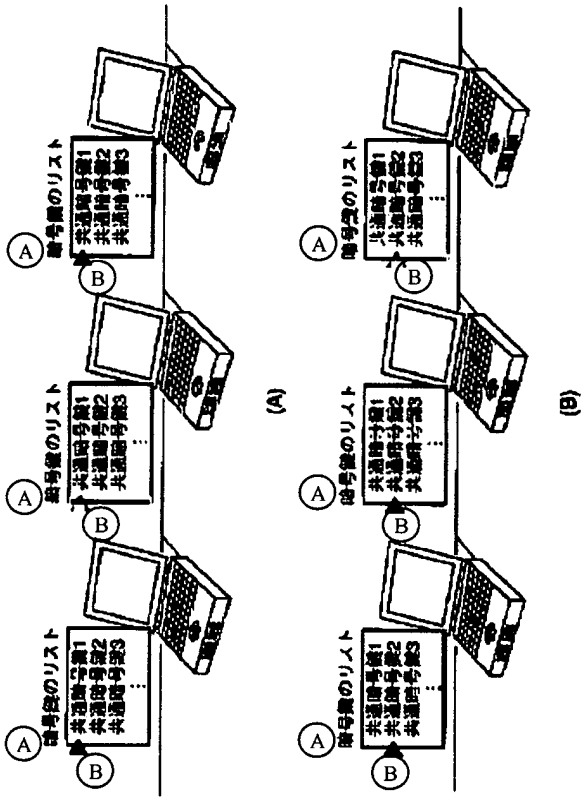


Figure 2

Key: A Encryption key list
B Common encryption key __

[There are no amendments to this patent.]

Claims

1. For an encryption key update system of a communication system wherein multiple devices mutually exchange data while encrypting and decrypting the data by a common key method that uses the same encryption key for encryption and decryption,
an encryption key update system characterized in that each of the aforementioned devices is equipped with
a list holding means that holds an electronic encryption key list in which multiple encryption keys are recorded,
and a selection means that, based on a preset rule, selects one or more encryption keys from the multiple encryption keys recorded on the encryption key list held in the aforementioned list holding means.

2. The encryption key update system recorded in Claim 1, characterized in that each of the aforementioned devices has
a validity period calculation means that, based on a preset rule, calculates a validity period for an encryption key selected by the aforementioned selection means,
and an encryption key update means that causes the aforementioned selection means to select a new encryption key when the time period from the selection of an encryption key by the aforementioned selection means to the [end of the] period calculated by the aforementioned validity period calculation means has elapsed.

3. The encryption key update system recorded in Claim 1 or 2, characterized in that the aforementioned selection means reselects at least one [encryption key] from the encryption keys selected the previous time.

4. The encryption key update system recorded in Claim 1 or 2, characterized in that each of the aforementioned devices
is equipped with a time difference adjustment means that, for only a prescribed period of time subsequent to the selection of an encryption key by the aforementioned selection means, adds the encryption key prior to that selection as a candidate encryption key for decryption use.

5. The encryption key update system recorded in Claim 1, 2, 3, or 4, characterized in that each of the aforementioned devices is equipped with a list reception means that receives the aforementioned encryption key list, and a list update means that updates the encryption key list held in the aforementioned list holding means with the encryption key list received by the aforementioned list reception means.

6. For an encryption key update method for a communication system wherein multiple devices mutually exchange data while encrypting and decrypting the data by a common key method that uses the same encryption key for encryption and decryption,
an encryption key update method characterized in that each of the aforementioned devices has [sic; possibly, executes]
a step wherein an electronic encryption key list in which multiple encryption keys are recorded is held,
and a step wherein one or more encryption keys from the multiple encryption keys recorded on the encryption key list that is held is/are selected based on a preset rule.

7. The encryption key update method recorded in Claim 6, characterized in that each of the devices has
a step wherein a validity period for an encryption key selected by the aforementioned selection means is calculated based on a preset rule,

and a step wherein a new encryption key is selected when the time period from the selection of the aforementioned encryption key to the [end of the] aforementioned calculated period has elapsed.

8. The encryption key update method recorded in Claim 6 or 7, characterized in that the aforementioned selection step reselects at least one [encryption key] from the encryption keys selected the previous time.

9. The encryption key update method recorded in Claim 6 or 7, characterized in that each of the aforementioned devices has
a step wherein, for only a prescribed period of time subsequent to the selection of an encryption key, the encryption key prior to that selection is added as a candidate encryption key for decryption use.

10. The encryption key update method recorded in Claim 6, 7, 8, or 9, characterized in that each of the aforementioned devices
has a step wherein the aforementioned encryption key list is received,
and a step wherein the aforementioned encryption key list that is being held is updated with the aforementioned received encryption key list.

Detailed explanation of the invention

[0001]

Technical field of the invention

The present invention pertains to an encryption key update system and an encryption key update method for a communication system wherein data are transmitted and received via wireless communication lines, for example; in particular, it pertains to an encryption key update system and an encryption key update method that enable the encryption key for all devices that are transmitting and receiving data to be updated synchronously without requiring complicated operations such as the setting and input of an encryption key on the part of the user.

[0002]

Prior art

In recent years there has been remarkable improvement in data communication technology, and communication systems known as the internet and intranets have rapidly spread. In addition, recently many businesses have established within their offices wireless LANs (Local Area Networks), which transmit and receive data by means of infrared light or radio waves. These wireless LANs do not require the laying of cables; therefore, they are flexible with respect to the handling of change in office layout due to a restructuring of the organization, for example.

[0003]

With wireless communication that transmits data with infrared light or radio waves, leakage of that [data] easily occurs, so countermeasures to prevent data from being intercepted or counterfeited by a third party are considered even more critical than with wired communication. Therefore, conventionally data encryption methods are widely used. Currently this data encryption primarily involves (1) a common encryption key method or (2) a public encryption key method, or a combination of the two.

[0004]

The common encryption key method is a method whereby the transmitting side (the side that encrypts the data) and the receiving side (the side that decrypts the encrypted data) are provided with a common encryption key in advance, with both the encryption and decryption being performed using the same encryption key. On the other hand, with the public encryption key method, two types of keys, a public key and a private key, are generated from a given key, and the public key is distributed in advance to the transmitting side. Then, the transmitting side encrypts the data using this public key, and the receiving side performs decryption with a private key that is paired with this public key. Furthermore, the combination of this common encryption key method and pubic encryption key method [results in a method whereby] the common encryption key of a common encryption key method is transferred by means of a public encryption key method.

[0005]

Thus it is possible to prevent the interception or counterfeiting of data by performing data encryption and decryption using a common encryption key or a public key and a private key.

[0006]

Furthermore, recently a strong demand has developed for the ability to access a company-internal LAN from a remote location such as a trip destination, and to respond to this demand, companies such as Canada's Border Network Technologies Corporation and Network Dynamics, Inc. of the U.S. have developed user verification systems known as one-time password systems.

[0007]

These one-time password systems do not encrypt data; rather, they are systems that increase network security by verifying whether a user who is accessing from a remote location is a valid user, providing a means by which the side being accessed and the side doing the accessing – for example, a firewall on the network side and an expansion unit connected to a

mobile computer – are made to generate the same random number simultaneously. Then, the user inputs the random number, which is generated/updated once per minute, as a password into an input device of the expansion unit, and if that password is recognized, access to the network is permitted.

[0008]

In other words, with these one-time password systems, each password is a single-use password, so it is not necessary to be concerned about theft of the password.

[0009]

Problems to be solved by the invention

However, with data encoding by means of the aforementioned common encryption key method, if the same key is used continuously for a long time, the danger that that code will be stolen increases. Therefore, work is required to update the key at given intervals.

[0010]

However, for example, a wireless LAN encryption key in the IEEE802.11b standard can be set within 40 bits or within 128 bits, and when an attempt is made to distribute/set a new encryption key comprised of 128 bits, the operation is extremely complicated. In addition, [the operation] is performed manually, so there is a risk that setting mistakes may occur or that the password may be leaked.

[0011]

Furthermore, with data encryption with a public encryption key method or data encryption with a combination of a common encryption key method and a public encryption key method, there is a problem in that it is too difficult to perform the [required] processing at the lower layers of the network, such as the hardware and firmware [layer], so implementation is difficult. Furthermore, even if implementation were achieved, there would be a problem in that the communication capability would be severely reduced.

[0012]

On the other hand, a one-time password system is a method that changes the password with each use, so it is not necessary to update the key at given intervals, as with data encryption with the common encryption key method. However, this one-time password system has the same problem, in that the random numbers generated by the system must be input each time by the user.

[0013]

The present invention was devised in response to problems of this type, the objective being to provide an encryption key update system and an encryption key update method that enable the encryption keys for all devices that are transmitting and receiving data to be updated synchronously without requiring complicated operations such as the setting and input of an encryption key on the part of the user.

[0014]

Means to solve the problems

To achieve the aforementioned objective, the present invention is one whereby one year's worth of encryption keys, for example, are distributed in advance to all of the devices, and each device uses the same rule as the other devices to select an encryption key therefrom for use in encryption and decryption. In addition, for that purpose, the present invention provides an encryption key update system that is an encryption key update system of a communication system wherein multiple devices mutually exchange data while encrypting and decrypting the data by a common key method that uses the same encryption key for encryption and decryption, being characterized in that each of the aforementioned devices is equipped with a list holding means that holds an electronic encryption key list in which multiple encryption keys are recorded, and a selection means that, based on a preset rule, selects one or more encryption keys from the multiple encryption keys recorded on the encryption key list held in the aforementioned list holding means.

[0015]

With the encryption key update system of the present invention, each device selects – based on a prescribed rule – an encryption key for use in encryption and decryption from the multiple encryption keys provided in advance; therefore, all of the devices are able to update the encryption key automatically and synchronously, and the user does not have to perform complicated operations such as the setting and input of an encryption key.

[0016]

Furthermore, with the encryption key update system of the present invention, it is preferable that each of the aforementioned devices have a validity period calculation means that, based on a preset rule, calculates a validity period for an encryption key selected by the aforementioned selection means, and an encryption key update means that causes the aforementioned selection means to select a new encryption key when the time period from the

selection of an encryption key by the aforementioned selection means to the [end of the] period calculated by the aforementioned validity period calculation means has elapsed. Thus, it is possible to provide an irregular update cycle, enabling security to be further improved.

[0017]

Furthermore, with the encryption key update system of the present invention, it is preferable that the aforementioned selection means reselect at least one [encryption key] from the encryption keys selected the previous time. Thus, for example, at least one [encryption key] before the update and after the update will match, and the transmission/reception of data will not be interrupted when the encryption key is updated.

[0018]

Furthermore, with the encryption key update system of the present invention it is preferable that each of the aforementioned devices be equipped with a time difference adjustment means that, for only a prescribed period of time subsequent to the selection of an encryption key by the aforementioned selection means, adds the encryption key prior to that selection as a candidate encryption key for decryption use. Thus, discrepancies in the encryption key update timing between the multiple devices can be handled within an appropriate range.

[0019]

Furthermore, with the encryption key update system of the present invention, it is preferable that each of the aforementioned devices be equipped with a list reception means that receives the aforementioned encryption key list, and a list update means that updates the encryption key list held in the aforementioned list holding means with the encryption key list received by the aforementioned list reception means. Thus, after the encryption key list is distributed initially and the system is started up, this encryption key list itself can be encrypted and transmitted/received, after which the distribution or setting of the encryption key list by the user is completely unnecessary.

[0020]

Embodiment of the invention

In the following an embodiment of the present invention will be explained with reference to the figures.

[0021]

Figure 1 is a network configuration diagram for a communication system to which an encryption key update system according to an embodiment of the present invention is applied.

[0022]

As shown in Figure 1, with this communication system, a network management server computer 1 and multiple access points 2 are connected to a wired LAN 100. In addition, each access point 2 establishes a wireless communication path with a personal computer 3 using infrared light, radio waves, or the like.

[0023]

Network management server computer 1 manages this entire communication system and, for example, distributes the encryption key list, to be explained later. Furthermore, the access points 2 are devices for the purpose of connecting personal computers 3 to wired LAN 100; they possess the same encryption key as personal computers 3, and they exchange data with personal computers 3 while encrypting and decrypting the data with this encryption key – in other words, while performing encryption with a common encryption key method.

[0024]

As many as four of these encryption keys, which are shared between these access points 2 and personal computers 3, can be set at one time, for example, and when multiple encryption keys have been set, the transmitting side performs encryption using one of these. At this time the receiving side stores in a packet information indicating the sequence number [of the key] used to perform the encryption, and then transmits [said information]. The receiving side uses the encryption key indicated by the information stored in this packet to perform decryption.

[0025]

In addition, this encryption key update system that is applied to a communication system is characterized in that the encryption key(s) shared by these access points 2 and personal computers 3 can be updated synchronously without requiring complicated operations such as the setting and input of an encryption key on the part of the user, and this point will be explained in detail in the following.

[0026]

Figure 2 is a schematic diagram of the updating of an encryption key implemented with this encryption key update system.

[0027]

With this encryption key update system, an encryption key list on which are recorded multiple encryption keys is distributed in advance to all of the devices that perform data encryption with the common encryption key method – more specifically, to all of the access points 2 and personal computers 3. Then, a program that selects one or more encryption keys from this encryption key list based on a prescribed rule also is distributed to each device.

[0028]

For example, as shown in Figure 2(A), for a given period, each device selects 'common encryption key 1' as the encryption key, and automatically sets that key in the communication environment. Subsequently, as shown in Figure 2(B), with a given date and time as the boundary, each device discards that 'common encryption key 1' and selects 'common encryption key 2' as the encryption key, which it automatically sets in the communication environment.

[0029]

In other words, the result is that the encryption key of each device is updated synchronously and security can be increased; in addition, the user is not forced to perform complicated operations such as the setting and input of an encryption key.

[0030]

Figure 3 is a block diagram showing the structure of the encryption key update system with which each device that forms this communication system is provided.

[0031]

As for the structures pertaining to this encryption key system, both the access points 2 and personal computers 3 are provided with the same components, so an example of a personal computer 3 will be explained.

[0032]

Personal computer 3 has a CPU 31, a system memory 32, a floppy disk device 33, a magnetic disk device 34, and a wireless signal transmitter/receiver 35.

[0033]

CPU 31 provides overall control for personal computer 3, controlling this personal computer 3 as defined by a wireless LAN transmission/reception control program 311, an encryption key management program 312, an update program 313, and the like.

[0034]

System memory 32 is a memory device that serves as the main memory for this personal computer 3, and is used to store the encryption key 321 that is actually used at the time for data encryption and decryption.

[0035]

Floppy disk device 33 and magnetic disk device 34 are memory devices that serve as external memory for this personal computer 3, and floppy disk device 33 is used to read an encryption key list 341, to be explained later, that is stored on a floppy disk for distribution use. Magnetic disk device 34 is used to store the encryption key list 341 that is read from the floppy disk by floppy disk device 33. This encryption key list 341 is the encryption key list that was explained with reference to Figure 2, and on which multiple encryption keys are recorded in advance.

[0036]

Wireless signal transmitter/receiver 35 transmits infrared signals to an access point 2 or receives infrared signals transmitted from an access point 2 to transport data.

[0037]

Next, a case wherein this personal computer 3 transmits data to an access point 2 via wireless signal transmitter/receiver 35 and a case wherein data from an access point 2 is received via wireless signal transmitter/receiver 35 will be considered.

[0038]

When data are transmitted, wireless LAN transmission/reception control program 311 encrypts the data using any of the encryption keys 321 stored in system memory 32, and these encrypted data are transmitted to access point 2 via wireless signal transmitter/receiver 35. At this time, information indicating the sequence number of the encryption key 321 that was used is stored in a packet. On the other hand, when data are received, to decrypt the data, wireless LAN transmission/reception control program 311 uses the encryption key 321 – of the encryption keys stored in system memory 32 – whose number is specified by the packet.

[0039]

In other words, it can be seen that encryption keys 321 stored in system memory 32 are extremely critical in the transmission and reception of data between personal computer 3 and access point 2.

[0040]

Accordingly, the updating of these encryption keys 321, which is executed by encryption key management program 312, will be explained next.

[0041]

First, a first operating principle with respect to the updating of encryption keys by means of this encryption key management program 312 will be explained with reference to Figure 4.

[0042]

Assume that multiple encryption keys (1)-(n) are recorded in encryption key list 341 and encryption keys (1)-(4) are initially set in system memory 32 as encryption keys 321.

[0043]

After a given period of time has elapsed, based on a prescribed rule, encryption key management program 312 selects the pre-existing encryption key (1) from the encryption keys 321 in system memory 32, and selects encryption keys (5)-(7) from encryption key list 341 in magnetic disk device 34, and resets these as the new encryption keys 321 in system memory 32.

[0044]

When a given period of time again has elapsed, based on a prescribed rule, encryption key management program 312 selects the pre-existing encryption key (5) from the encryption keys 321 in system memory 32, and selects encryption keys (18)-(20) from encryption key list 341 in magnetic disk device 34, and resets these as the new encryption keys 321 in system memory 32.

[0045]

In the same manner, when a given period of time again has elapsed, based on a prescribed rule, encryption key management program 312 selects the pre-existing encryption key (19) from the encryption keys 321 in system memory 32, and selects encryption keys (32)-(34) from

encryption key list 341 in magnetic disk device 34, and resets these as the new encryption keys 321 in system memory 32.

[0046]

In other words, encryption key management program 312 makes one of the four encryption keys after the update a duplicate of [one of the keys] before the update, and thus prevents the interruption of data transmission/reception when these encryption keys are updated.

[0047]

As for the selection rule, encryption key management program 312 can select encryption keys in order from the end of encryption key list 341, but security can be further increased by providing irregularity to that order. As a method for providing this irregularity, for example, the system time for personal computer 3 can be obtained and a preset function calculation can be executed based on the obtained system time to determine the encryption keys to be selected.

[0048]

Furthermore, encryption key management program 312 can perform this encryption key update at preset time intervals, but security can be further increased by providing irregularity to that cycle. As a method for providing this irregularity, for example, the system time for personal computer 3 can be obtained and a preset function calculation can be executed based on the obtained system time to determine the validity period for each encryption key.

[0049]

Next, a second operating principle with respect to the updating of encryption keys by means of this encryption key management program 312 will be explained with reference to Figure 5.

[0050]

Assume that encryption keys (1)-(n) are recorded in encryption key list 341 and encryption keys (1)-(2) are initially set in system memory 32 as encryption keys 321. In other words, two encryption keys, which is half of the number of four [keys] that can be set at one time, have been set.

[0051]

After a given period of time has elapsed, based on a prescribed rule, encryption key management program 312 selects encryption keys (5)-(6) from encryption key list 341 in magnetic disk device 34, and resets these as the new encryption keys 321 in system memory 32.

[0052]

In response thereto, wireless LAN transmission/reception control program 311 takes the two encryption keys (5)-(6) as candidate encryption keys to be used when data are encrypted. However, for only a prescribed period of time subsequent to the update of these encryption keys, wireless LAN transmission/reception control program 311 adds pre-update encryption keys (1)-(2) to the two encryption keys (5)-(6) as candidates for data decryption use, bringing the total number of keys to four.

[0053]

When a given period of time again has elapsed, based on a prescribed rule, encryption key management program 312 selects encryption keys (18)-(19) from encryption key list 341 in magnetic disk device 34, and resets these as the new encryption keys 321 in system memory 32. In response thereto wireless LAN transmission/reception control program 311 takes the two encryption keys (18)-(19) as candidate encryption keys to be used when data are encrypted and, for only a prescribed period of time subsequent to the update of these encryption keys, adds the pre-update encryption keys (5)-(6) to the two encryption keys (18)-(19) as candidates for data decryption use, bringing the total number of keys to four.

[0054]

In the same manner, when a given period of time again has elapsed, based on a prescribed rule, encryption key management program 312 selects encryption keys (32)-(33) from encryption key list 341 in magnetic disk device 34, and resets these as the new encryption keys 321 in system memory 32, and wireless LAN transmission/reception control program 311 takes the two encryption keys (32)-(33) as candidate encryption keys to be used when data are encrypted and, for only a prescribed period of time subsequent to the update of these encryption keys, adds the pre-update encryption keys (18)-(19) to the two encryption keys (32)-(33) as candidates for data decryption use, bringing the total number of keys to four.

[0055]

In other words, encryption key management program 312 is executed without duplicating a pre-update encryption key after the update, but wireless LAN transmission/reception control

program 311 permits [the use of] pre-update encryption keys for only a prescribed period of time, and thus discrepancies in the encryption key update timing between the multiple devices can be handled within an appropriate range. For this purpose, encryption key management program 312 makes the number of encryption keys one half or less of the number that can be handled at one time.

[0056]

Thus, with this encryption key update system, one year's worth of encryption keys, for example, is distributed in advance to all of the devices, and each device uses the same rule as the other devices to select an encryption key therefrom for use in encryption and decryption; therefore, the encryption keys for all of the devices performing data transmission/reception can be updated synchronously without requiring complicated operations such as the setting and input of an encryption key on the part of the user.

[0057]

Next, the operating procedures for this encryption key update system will be explained with reference to Figure 6 and Figure 7.

[0058]

Figure 6 is a flowchart for the purpose of explaining the operating procedure of encryption key management program 312.

[0059]

Encryption key management program 312 first obtains the system time for personal computer 3 (step A1). When the system time is obtained, encryption key management program 312 executes a function calculation that has been provided in advance based on the obtained system time and selects new encryption keys from encryption key list 341 stored in magnetic disk device 34 (step A2).

[0060]

When the new encryption keys are selected, encryption key management program 312 sets the selected encryption keys in system memory 32 as encryption keys 321 (step A3). Then, based on the previously obtained system time, encryption key management program 312 executes a function calculation provided in advance for the purpose of calculating the validity period, and thus calculates the validity period for the new encryption keys (step A4).

[0061]

Finally, encryption key management program 312 sets a startup timer for the purpose of restarting itself after the calculated validity period [has elapsed] (step A5), and the process is complete.

[0062]

Figure 7 is a flowchart for the purpose of explaining the operating procedure for decryption by wireless LAN transmission/reception control program 311.

[0063]

When wireless LAN transmission/reception control program 311 receives data from an access point 2 via wireless signal transmitter/receiver 35, it attempts to decrypt these data using the encryption key – of the encryption keys set in system memory 32 – whose number is specified by the packet (step B1).

[0064]

When this decryption succeeds (YES in step B2), the decryption process of wireless LAN transmission/reception control program 311 is complete; however, if it fails (NO in step B2), wireless LAN transmission/reception control program 311 checks whether [the current time] is within the preset period of time after the update of the encryption keys 321 that are set in system memory 32 (step B3).

[0065]

If it is within the preset period of time (YES in step B3), wireless LAN transmission/reception control program 311 next attempts to decrypt these data using the old encryption key – of the old, pre-update encryption keys – whose number is specified by the packet (step B4).

[0066]

Then, if the decryption succeeds (YES in step B7 [sic; B5]), decryption by wireless LAN transmission/reception control program 311 is complete; however, if it fails (NO in step B5), or if it is not within the prescribed period of time after the update of the encryption keys 321 (NO in step B3), wireless LAN transmission/reception control program 311 transmits an error response to the access point 2 (step B6).

[0067]

In addition, the operating procedure for decryption by wireless LAN transmission/reception control program 311 shown in Figure 7 is [used] when encryption key management program 312 updates the encryption keys based on the second operating principle shown in Figure 5; when encryption key management program 312 updates the encryption keys based on the first operating principle shown in Figure 4 and the decryption in step B2 fails, the error response of step B6 can be transmitted.

[0068]

Furthermore, after encryption key list 341 is distributed and the system is started up, this encryption key list 341 itself can be encrypted and then transmitted and received. Therefore, the subsequent storage of encryption key list 341 on a floppy disk for distribution, and the distribution thereof, and the reading [of the list] by floppy disk device 33 of each device and the setting [of encryption keys] become completely unnecessary. Therefore, with this encryption key update system, an update program 313 is provided.

[0069]

When the encryption key list transmitted from network management server computer 1 is received by wireless signal transmitter/receiver 35, first, wireless LAN transmission/reception control program 311 decrypts the encryption key list encrypted by access point 2. Next, this decrypted encryption key list is transmitted to update program 313, and the encryption key list 341 in magnetic disk device 34 is updated by means of update program 313.

[0070]

Furthermore, to increase security, it is effective to provide this update program 313 with the update function of encryption key management program 312. In other words, after a new encrypted encryption key management program is transmitted from network management server computer 1 and this new encrypted encryption key management program is decrypted by wireless LAN transmission/reception control program 311, update program 313 is made to update encryption key management program 312. Thus, the encryption key selection rules also can be updated without manual intervention, and the risk of theft of the code can be reduced.

[0071]

Effect of the invention

As explained above, by means of the present invention, system one year's worth of encryption keys, for example, is distributed in advance to all of the devices, and each device uses

the same rule as the other devices to select an encryption key therefrom for use in encryption and decryption; consequently, the encryption keys for all of the devices performing data transmission/reception can be updated automatically and synchronously without requiring complicated operations such as the setting and input of an encryption key on the part of the user.

[0072]

Furthermore, by making the encryption key update cycle irregular, security can be further increased.

[0073]

Furthermore, by using at least one encryption key after an update that is a duplicate of a pre-update [encryption key], or by adding a pre-update encryption key as a candidate encryption key for decryption use for only a prescribed period of time, it is possible to prevent the interruption of data transmission/reception when the encryption keys are updated, or to handle discrepancies in the encryption key update timing between the multiple devices within an appropriate range.

Brief description of the figures

Figure 1 is a network configuration diagram for a communication system to which an encryption key update system according to an embodiment of the present invention is applied.

Figure 2 is a schematic diagram of the updating of an encryption key implemented with the encryption key update system of said embodiment.

Figure 3 is a block diagram showing the structure of the encryption key update system with which each device that forms the communication system of said embodiment is provided.

Figure 4 is a diagram for the purpose of explaining a first operating principle with respect to the updating of an encryption key by means of the encryption key management program of said embodiment.

Figure 5 is a diagram for the purpose of explaining a second operating principle with respect to the updating of an encryption key by means of the encryption key management program of said embodiment.

Figure 6 is a flowchart for the purpose of explaining the operating procedure of the encryption key management program of said embodiment.

Figure 7 is a flowchart for the purpose of explaining the operating procedure for decryption by a wireless LAN transmission/reception control program of said embodiment.

Explanation of symbols

1 Network management server computer
2 Access point
3 Personal computer
31 CPU
32 System memory
33 Floppy disk
34 Magnetic disk device
35 Wireless signal transmitter/receiver
100 Wired LAN
311 Wireless LAN transmission/reception control program
312 Encryption key management program
313 Update program
321 Encryption key
341 Encryption key list

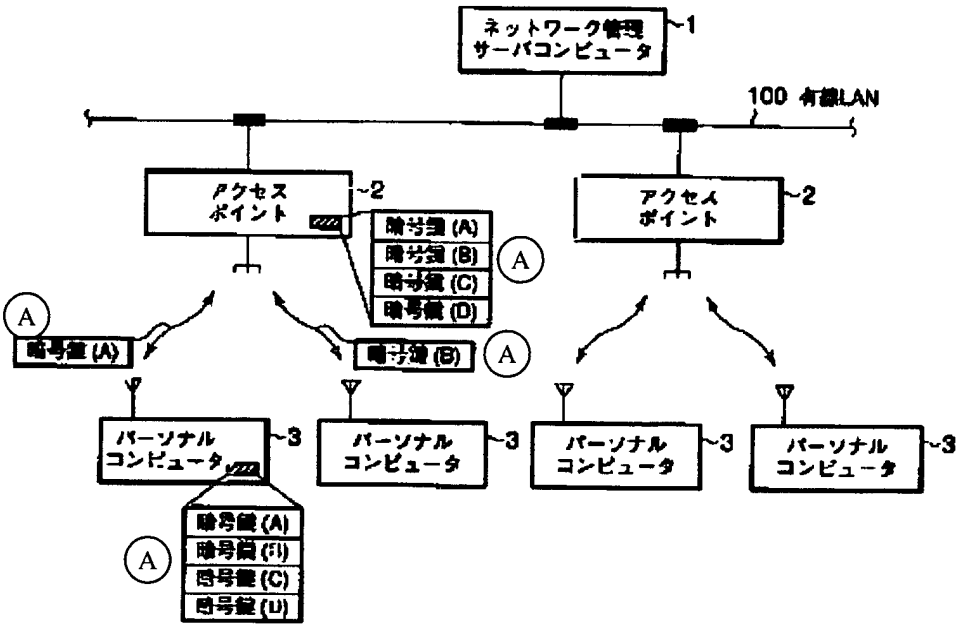


Figure 1

Key: 1 Network management server computer
2 Access point
3 Personal computer
100 Wired LAN
A Encryption key ___

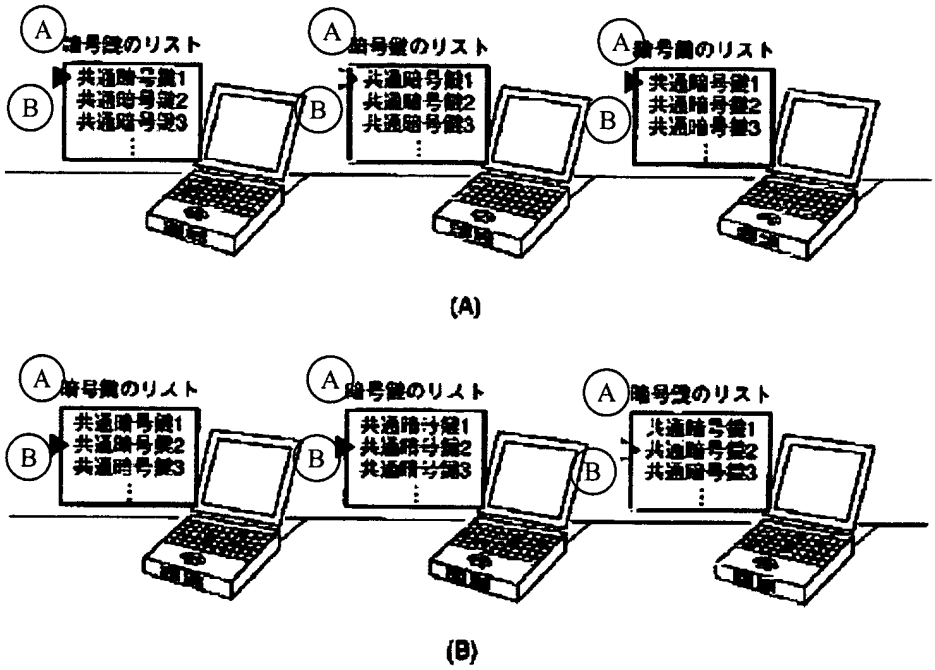


Figure 2

Key: A Encryption key list
B Common encryption key __

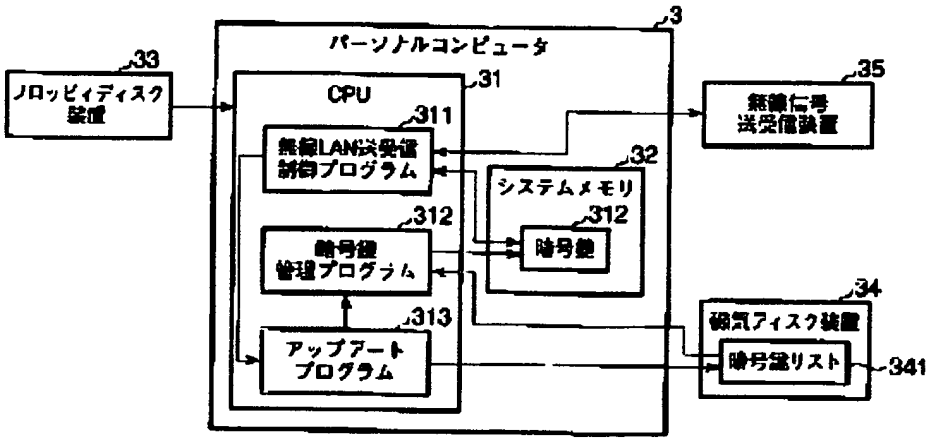


Figure 3

Key: 3 Personal computer
31 CPU
32 System memory
33 Floppy disk device
34 Magnetic disk device
35 Wireless signal transmitter/receiver

311 Wireless LAN transmission/reception control program
312 Encryption key control program
313 Update program
312 [sic; 321] Encryption key
341 Encryption key list

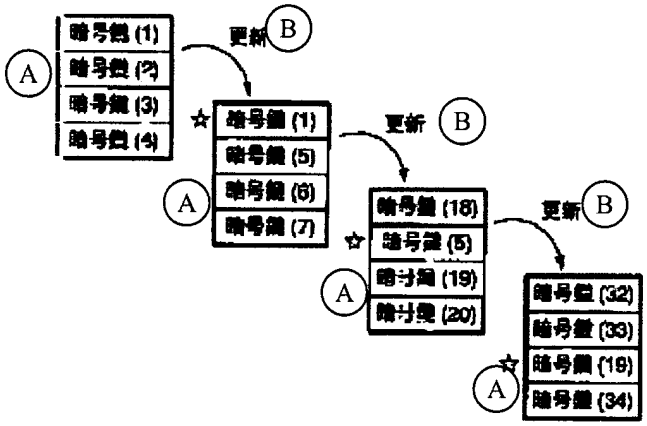


Figure 4

Key: A Encryption key __
B Update

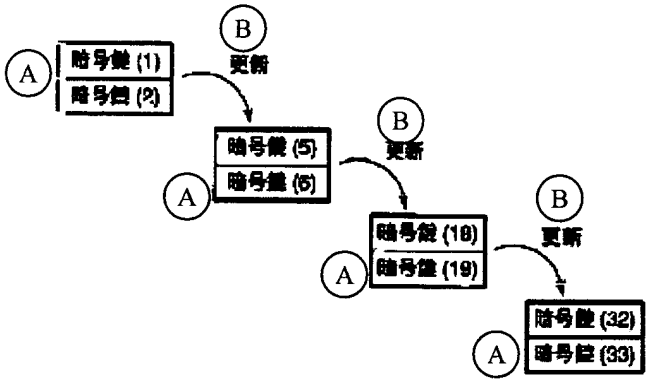


Figure 5

Key: A Encryption key __
B Update

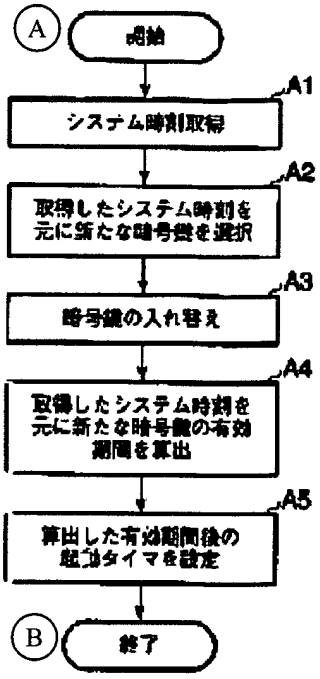


Figure 6

Key:
- A Start
- B End
- A1 Obtain system time
- A2 Select new encryption keys based on obtained system time
- A3 Replace encryption keys
- A4 Calculate validity period for new encryption keys based on obtained system time
- A5 Set startup timer [for restart] after calculated validity period

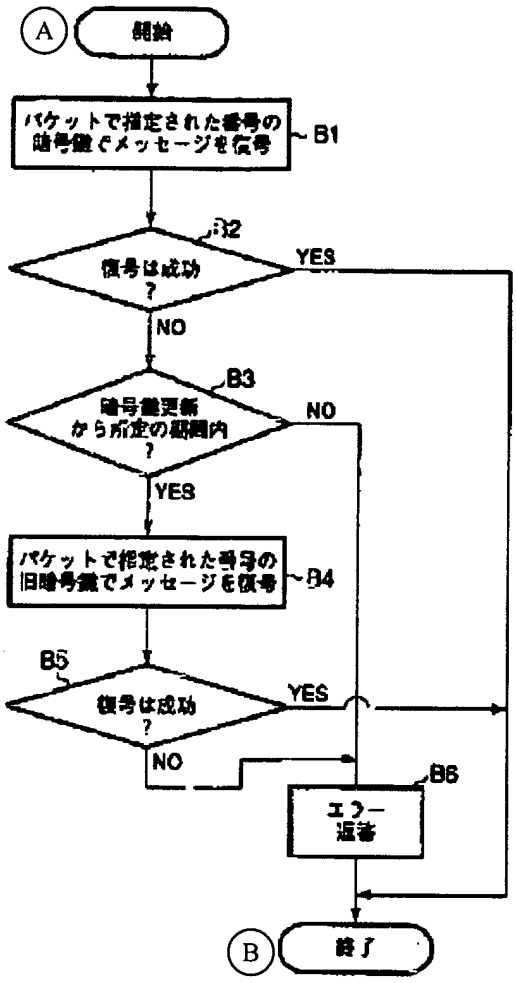


Figure 7

Key:
- A Start
- B End
- B1 Decrypt message with encryption key whose number is specified by packet
- B2 Decryption successful?
- B3 Is [current time] within prescribed time period subsequent to encryption key update?
- B4 Decrypt message with old encryption key whose number is specified by packet
- B5 Decryption successful?
- B6 Transmit error

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－290396
（P2002－290396A）
(43)公開日　平成14年10月４日(2002.10.4)

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
H04L 9/16		H04L 9/00	643	5J104
9/08			601E	

審査請求　未請求　請求項の数10　ＯＬ　（全 9 頁）

(21)出願番号　特願2001－85823(P2001－85823)

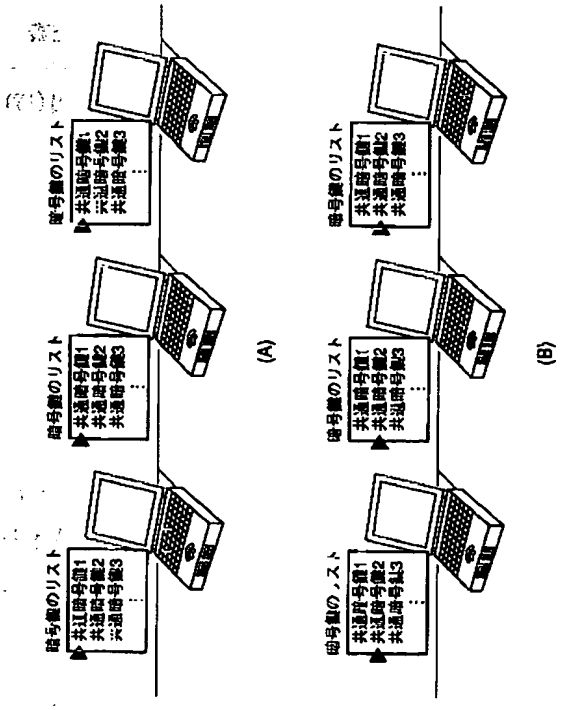
(22)出願日　平成13年３月23日(2001.3.23)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　鈴木　昇
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5J104 AA01 AA16 AA34 EA04 EA24
JA03 NA02 PA07

(54)【発明の名称】　暗号鍵更新システムおよび暗号鍵更新方法

(57)【要約】
【課題】ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることなく、データを送受信するすべての装置の暗号鍵を同期的に更新することを可能とした暗号鍵更新システム。
【解決手段】この暗号鍵更新システムでは、共通暗号鍵方式によるデータの暗号化を行うすべての装置に、予め複数の暗号鍵が記された暗号鍵リストを配布しておく。また、各装置には、所定の規則に基づき、この暗号鍵リストの中から１つ以上の暗号鍵を選択するプログラムも配布しておく。そして、たとえば、ある期間、各装置は、「共通暗号鍵１」を暗号鍵として選択し、それを通信環境に自動設定する。その後、ある日時を境に、各装置は、その「共通暗号鍵１」を破棄して「共通暗号鍵２」を暗号鍵として選択し、それを通信環境に自動設定する。



【特許請求の範囲】
【請求項１】　暗号化と復号とに同一の暗号鍵を用いる共通鍵方式によりデータを暗号化および復号しながら複数の装置が互いにデータを送受信する通信システムの暗号鍵更新システムであって、
前記各装置が、
複数の暗号鍵が記された電子的な暗号鍵リストを保持するリスト保持手段と、
予め定められた規則に基づき、前記リスト保持手段に保持された暗号鍵リストに記される複数の暗号鍵の中から１つ以上の暗号鍵を選択する選択手段とを具備したことを特徴とする暗号鍵更新システム。
【請求項２】　前記各装置が、
予め定められた規則に基づき、前記選択手段により選択された暗号鍵の有効期間を算出する有効期間算出手段と、
前記選択手段により暗号鍵が選択された時から前記有効期間算出手段により算出された期間が経過した時に、前記選択手段に新たな暗号鍵を選択させる暗号鍵更新手段とを具備したことを特徴とする請求項１記載の暗号鍵更新システム。
【請求項３】　前記選択手段は、前回選択した暗号鍵の中の少なくとも１つを再度選択することを特徴とする請求項１または２記載の暗号鍵更新システム。
【請求項４】　前記各装置が、
前記選択手段により暗号鍵が選択された時から予め定められた期間内に限り、その更新前の暗号鍵を復号用の暗号鍵の候補に加える時差調整手段を具備することを特徴とする請求項１または２記載の暗号鍵更新システム。
【請求項５】　前記各装置が、
前記暗号鍵リストを受信するリスト受信手段と、
前記リスト保持手段に保持された暗号鍵リストを前記リスト受信手段により受信された暗号鍵リストに更新するリスト更新手段とを具備することを特徴とする請求項１、２、３または４記載の暗号鍵更新システム。
【請求項６】　暗号化と復号とに同一の暗号鍵を用いる共通鍵方式によりデータを暗号化および復号しながら複数の装置が互いにデータを送受信する通信システムの暗号鍵更新方法であって、
前記各装置が、
複数の暗号鍵が記された電子的な暗号鍵リストを保持するステップと、
予め定められた規則に基づき、前記保持した暗号鍵リストに記される複数の暗号鍵の中から１つ以上の暗号鍵を選択するステップとを有することを特徴とする暗号鍵更新方法。
【請求項７】　前記各装置が、
予め定められた規則に基づき、前記選択された暗号鍵の有効期間を算出するステップと、
前記暗号鍵を選択した時から前記算出された期間が経過した時に、新たな暗号鍵を選択するステップとを有することを特徴とする請求項６記載の暗号鍵更新方法。
【請求項８】　前記選択ステップは、前回選択した暗号鍵の中の少なくとも１つを再度選択することを特徴とする請求項６または７記載の暗号鍵更新方法。
【請求項９】　前記各装置が、
前記暗号鍵を選択した時から予め定められた期間内に限り、その更新前の暗号鍵を復号用の暗号鍵の候補に加えるステップを有することを特徴とする請求項６または７記載の暗号鍵更新方法。
【請求項１０】　前記各装置が、
前記暗号鍵リストを受信するステップと、
前記保持した暗号鍵リストを前記受信した暗号鍵リストに更新するステップとを有することを特徴とする請求項６、７、８または９記載の暗号鍵更新方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、たとえば無線通信回線を介してデータを送受信する通信システムの暗号鍵更新システムおよび暗号鍵更新方法に係り、特に、ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることなく、データを送受信するすべての装置の暗号鍵を同期的に更新することを可能とした暗号鍵更新システムおよび暗号鍵更新方法に関する。
【０００２】
【従来の技術】近年、データ通信技術の向上は目覚ましく、インターネットやイントラネットなどと称される通信システムが急速に普及している。また、最近では、赤外線や電波などによりデータを送受信する無線通信を利用した無線ＬＡＮ（Local AreaNetwork）をオフィス内に構築する企業も多くなってきている。この無線ＬＡＮは、ケーブルの敷設を必要としないために、たとえば組織の改編に伴うオフィス内のレイアウト変更などにも柔軟に対応することが可能である。
【０００３】赤外線や電波などにデータを搬送させる無線通信では、その漏洩を発生させ易いため、有線通信以上に、第３者によるデータの傍受や改ざん等を防ぐための対策が重要視される。このことから、従来より、データの暗号化という手法が広く採用されている。このデータの暗号化は、（１）共通暗号鍵方式、（２）公開暗号鍵方式のいずれか、あるいは、この２つの組み合わせによるものが現在のところ主流である。
【０００４】共通暗号鍵方式は、送信側（データを暗号化する側）と受信側（暗号化されたデータを復号する側）とが、予め共通の暗号鍵を持ち、この同一の暗号鍵を用いて暗号化および復号を行う方式である。一方、公開暗号鍵方式は、ある鍵から公開鍵と秘密鍵との２種類の鍵を生成し、公開鍵を予め送信側に配布しておく。そして、送信側は、この公開鍵を用いてデータを暗号化し、受信側は、この公開鍵と対になっている秘密鍵で復

号を実行する。また、この共通暗号鍵方式と公開暗号鍵方式との組み合わせは、共通暗号鍵方式における共通暗号鍵を公開暗号鍵方式によって授受するものである。

【０００５】このように、共通暗号鍵や公開鍵、秘密鍵を用いてデータの暗号化および復号を行うことにより、データの傍受や改ざんを防止することが可能となる。

【０００６】また、最近では、社内ＬＡＮに外出先等の遠隔地からアクセスしたいといった要望も多く、これに答えるために、たとえば加国ボーダー・ネットワーク・テクノロジー社や米国セキュリティダイナミクス社等がワンタイム・パスワード・システムと称されるユーザ認証システムを開発するに至っている。

【０００７】このワンタイム・パスワード・システムは、データを暗号化するものではないが、遠隔地からアクセスするユーザが正規のユーザかどうかを確認することによってネットワークのセキュリティを高めるためのシステムであり、たとえばネットワーク側のファイア・ウォールとモバイルコンピュータに接続される拡張ユニットなど、アクセスされる側とアクセスする側とで同じ時に同じ乱数を発生させる仕組みを持たせる。そして、ユーザは、たとえば１分ごとに発生・更新される乱数をパスワードとしてその拡張ユニットの入力装置に入力し、そのパスワードの承認を条件に、そのネットワークへのアクセスが許可される。

【０００８】つまり、このワンタイム・パスワード・システムでは、各パスワードがいわゆる使い捨てであるため、パスワードの盗難を考慮する必要がない。

【０００９】

【発明が解決しようとする課題】ところで、前述した共通暗号鍵方式によるデータの暗号化では、同じ鍵を長期間に渡って使い続けると、その暗号が破られる危険性が高くなってしまう。したがって、ある期間ごとに鍵を更新する作業が必要となってくる。

【００１０】しかしながら、たとえばＩＥＥＥ８０２．１１ｂ規格における無線ＬＡＮの暗号鍵は、４０ビット以内や１２８ビット以内での設定が可能であり、１２８ビットからなる暗号鍵を新たに配布・設定しようとすると、その作業は非常に煩雑である。そして、人手を介することから、たとえば設定ミスや暗号鍵自体の漏洩を誘発するおそれがあった。

【００１１】また、公開暗号鍵方式によるデータの暗号化や、共通暗号鍵方式と公開暗号鍵方式との組み合わせによる暗号化では、ハードウェアやファームウェアなど、ネットワークの下位層に処理をさせるには複雑すぎて実現困難であり、また、仮に実現できたとしても通信性能が著しく低下してしまうといった問題があった。

【００１２】一方、ワンタイム・パスワード・システムは、利用の度にパスワードを変える方式であるため、共通暗号鍵方式によるデータの暗号化のように、ある期間ごとに鍵を更新するといった作業は一切不要である。しかし、このワンタイム・パスワード・システムも、システムが発生させる乱数をその都度ユーザに入力させなければならないといった同様の問題を抱えている。

【００１３】この発明はこのような事情を考慮してなされたものであり、ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることなく、データを送受信するすべての装置の暗号鍵を同期的に更新することを可能とした暗号鍵更新システムおよび暗号鍵更新方法を提供することを目的とする。

【００１４】

【課題を解決するための手段】前述した目的を達成するために、この発明は、たとえば１年分の暗号鍵をすべての装置に予め配布しておき、各装置が、これらの中から暗号化および復号に用いる暗号鍵を他の装置と同じ規則で選択するようにしたものである。そして、そのために、この発明は、暗号化と復号とに同一の暗号鍵を用いる共通鍵方式によりデータを暗号化および復号しながら複数の装置が互いに情報を送受信する通信システムの暗号鍵更新システムであって、前記各装置が、複数の暗号鍵が記された電子的な暗号鍵リストを保持するリスト保持手段と、予め定められた規則に基づき、前記リスト保持手段に保持された暗号鍵リストに記される複数の暗号鍵の中から１つ以上の暗号鍵を選択する選択手段とを具備したことを特徴とする暗号鍵更新システムを提供する。

【００１５】この発明の暗号鍵更新システムにおいては、所定の規則に基づき、各装置が予め与えられた複数の暗号鍵の中から暗号化および復号に用いる暗号鍵を選択するため、その結果として、すべての装置が同期を取って暗号鍵を自動的に更新することが可能となり、ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることがない。

【００１６】また、この発明の暗号鍵更新システムは、前記各装置が、予め定められた規則に基づき、前記選択手段により選択された暗号鍵の有効期間を算出する有効期間算出手段と、前記選択手段により暗号鍵が選択された時から前記有効期間算出手段により算出された期間が経過した時に、前記選択手段に新たな暗号鍵を選択させる暗号鍵更新手段とを具備することが好ましい。これにより、暗号鍵の更新サイクルに不規則性を持たせることができ、セキュリティをより向上させることが可能となる。

【００１７】また、この発明の暗号鍵更新システムは、前記選択手段が、前回選択した暗号鍵の中の少なくとも１つを再度選択することが好ましい。これにより、たとえば更新前と更新後とで少なくとも１つは合致することになり、暗号鍵の更新時にもデータの送受信を中断させることがない。

【００１８】また、この発明の暗号鍵更新システムは、前記各装置が、前記選択手段により暗号鍵が選択された

時から予め定められた期間内に限り、その更新前の暗号鍵を復号用の暗号鍵の候補に加える時差調整手段を具備することが好ましい。これにより、複数の装置間での暗号鍵の更新タイミングのずれを適切な範囲内で吸収することが可能となる。

【００１９】また、この発明の暗号鍵更新システムは、前記各装置が、前記暗号鍵リストを受信するリスト受信手段と、前記リスト保持手段に保持された暗号鍵リストを前記リスト受信手段により受信された暗号鍵リストに更新するリスト更新手段とを具備することが好ましい。これにより、最初に暗号鍵リストを配布してシステムを起動させた後は、この暗号鍵リスト自体を暗号化して授受することができるようになり、以降、ユーザによる暗号鍵リストの配布や設定などを一切不要とすることが可能となる。

【００２０】

【発明の実施の形態】以下、図面を参照してこの発明の実施形態を説明する。

【００２１】図１は、この発明の実施形態に係る暗号鍵更新システムが適用される通信システムのネットワーク構成図である。

【００２２】図１に示すように、この通信システムは、有線ＬＡＮ１００にネットワーク管理サーバコンピュータ１と複数のアクセスポイント２とが接続される。また、各アクセスポイント２は、赤外線や電波などを利用して、パーソナルコンピュータ３との間に無線通信路を確立する。

【００２３】ネットワーク管理サーバコンピュータ１は、この通信システム全体の管理を司るものであり、後述する暗号鍵リストの配布などを実行する。また、アクセスポイント２は、パーソナルコンピュータ３を有線ＬＡＮ１００に接続するための装置であり、パーソナルコンピュータ３と同じ暗号鍵を保有し、この暗号鍵でデータの暗号化と復号とを行いながら、つまり共通暗号鍵方式による暗号化を行いながらパーソナルコンピュータ３との間でデータを送受信する。

【００２４】このアクセスポイント２とパーソナルコンピュータ３との双方に共有される暗号鍵は、たとえば４つまで一時に設定可能であり、複数の暗号鍵が設定された場合、送信側は、その中のどれかを用いて暗号化を行う。この時、送信側は、何番目の暗号鍵を使用したかを示す情報をパケットに格納して転送する。一方、受信側は、このパケットに格納された情報で示される番号の暗号鍵を用いて復号を実行する。

【００２５】そして、この通信システムに適用される暗号鍵更新システムは、このアクセスポイント２とパーソナルコンピュータ３との双方に共有される暗号鍵を、ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることなく、同期的に更新できるようにした点を特徴としており、以下、この点について詳述する。

【００２６】図２は、この暗号鍵更新システムで実行される暗号鍵の更新の概要を示すための概念図である。

【００２７】この暗号鍵更新システムでは、共通暗号鍵方式によるデータの暗号化を行うすべての装置、より具体的には、ここでは、すべてのアクセスポイント２およびパーソナルコンピュータ３に、予め複数の暗号鍵が記された暗号鍵リストを配布しておく。そして、各装置には、所定の規則に基づき、この暗号鍵リストの中から１つ以上の暗号鍵を選択するプログラムも配布しておく。

【００２８】たとえば図２（Ａ）に示すように、ある期間、各装置は、「共通暗号鍵１」を暗号鍵として選択し、それを通信環境に自動設定する。その後、図２（Ｂ）に示すように、ある日時を境に、各装置は、その「共通暗号鍵１」を破棄し、「共通暗号鍵２」を暗号鍵として選択し、それを通信環境に自動設定する。

【００２９】つまり、結果として、各装置の暗号鍵が同期的に更新されてセキュリティを高めることができ、かつ、ユーザに暗号鍵の入力や設定等の煩わしい作業を強いることもない。

【００３０】図３は、この通信システムを構成する各装置に備えられる暗号鍵更新システムに関わる構成を示すブロック図である。

【００３１】なお、この暗号鍵システムに関わる構成は、アクセスポイント２およびパーソナルコンピュータ３の双方に同じものが設けられるので、ここでは、パーソナルコンピュータ３を例に説明する。

【００３２】パーソナルコンピュータ３は、ＣＰＵ３１、システムメモリ３２、フロッピィディスク装置３３、磁気ディスク装置３４および無線信号送受信装置３５を有している。

【００３３】ＣＰＵ３１は、パーソナルコンピュータ３全体の制御を司るものであり、無線ＬＡＮ送受信制御プログラム３１１、暗号鍵管理プログラム３１２、アップデートプログラム３１３等の記述にしたがって、このパーソナルコンピュータ３を動作制御する。

【００３４】システムメモリ３２は、このパーソナルコンピュータ３の主記憶となるメモリデバイスであり、その時に実際にデータの暗号化および復号に用いられる暗号鍵３２１を格納するために利用される。

【００３５】フロッピィディスク装置３３および磁気ディスク装置３４は、このパーソナルコンピュータ３の外部記憶となるメモリデバイスであり、フロッピィディスク装置３３は、後述する暗号鍵リスト３４１が格納された頒布用のフロッピィディスクからこれらを読み出すために利用される。一方、磁気ディスク装置３４は、フロッピィディスク装置３３によりフロッピィディスクから読み出された暗号鍵リスト３４１を格納するために利用される。この暗号鍵リスト３４１は、図２を参照しながら説明した、予め複数の暗号鍵が記された暗号鍵リストである。

【００３６】そして、無線信号送受信装置３５は、データを搬送するための赤外線信号をアクセスポイント２に向けて送信し、あるいは、アクセスポイント２から送信された赤外線信号を受信するためのものである。

【００３７】ここで、このパーソナルコンピュータ３が、無線信号送受信装置３５を介してアクセスポイント２にデータを送信する場合、および、無線信号送受信装置３５を介してアクセスポイント２からデータを受信する場合を考える。

【００３８】データを送信する場合、無線ＬＡＮ送受信制御プログラム３１１は、システムメモリ３２に格納されたいずれかの暗号鍵３２１を用いてデータを暗号化し、この暗号化されたデータを無線信号送受信装置３５を介してアクセスポイント２に送信する。この時、何番目の暗号鍵３２１を使用したのかを示す情報をパケットに格納しておく。一方、データを受信する場合、無線ＬＡＮ送受信制御プログラム３１１は、システムメモリ３２に格納された暗号鍵３２１の中のパケットで指定される番号の暗号鍵３２１を用いてデータを復号する。

【００３９】つまり、このパーソナルコンピュータ３におけるアクセスポイント２との間のデータの送受信では、システムメモリ３２に格納された暗号鍵３２１の管理が非常に重要であることがわかる。

【００４０】そこで、次に、暗号鍵管理プログラム３１２が実行する、この暗号鍵３２１の更新について説明する。

【００４１】まず、図４を参照して、この暗号鍵管理プログラム３１２による暗号鍵の更新の第１の動作原理を説明する。

【００４２】いま、暗号鍵リスト３４１には、暗号鍵（１）～（ｎ）の複数の暗号鍵が記されており、また、システムメモリ３２には、当初、暗号鍵（１）～（４）が暗号鍵３２１として設定されているものと想定する。

【００４３】ある期間の経過後、暗号鍵管理プログラム３１２は、予め定められた規則に基づき、システムメモリ３２の暗号鍵３２１から既存の暗号鍵（１）と、磁気ディスク装置３４の暗号鍵リスト３４１から暗号鍵（５）～（７）とを選択し、これをシステムメモリ３２に新たな暗号鍵３２１として再設定する。

【００４４】さらにある期間の経過後、暗号鍵管理プログラム３１２は、予め定められた規則に基づき、システムメモリ３２の暗号鍵３２１から既存の暗号鍵（５）と、磁気ディスク装置３４の暗号鍵リスト３４１から暗号鍵（１８）～（２０）とを選択し、これをシステムメモリ３２に新たに暗号鍵３２１として再設定する。

【００４５】同様に、さらにある期間の経過後、暗号鍵管理プログラム３１２は、予め定められた規則に基づき、システムメモリ３２の暗号鍵３２１から既存の暗号鍵（１９）と、磁気ディスク装置３４の暗号鍵リスト３４１から暗号鍵（３２）～（３４）とを選択し、これをシステムメモリ３２に新たに暗号鍵３２１として再設定する。

【００４６】つまり、暗号鍵管理プログラム３１２は、４つの暗号鍵の中の１つは更新前と更新後とで重複させることにより、この暗号鍵の更新時にデータの送受信を中断させることを防止する。

【００４７】なお、この選択時の規則として、暗号鍵管理プログラム３１２は、暗号鍵リスト３４１の端から順番に暗号鍵を選択していってもよいが、その順番に不規則性を持たせれば、さらにセキュリティを高めることが可能である。この不規則性を持たせる方法としては、たとえばパーソナルコンピュータ３のシステム時刻を取得し、この取得したシステム時刻をもとに予め定められた関数演算を実行して選択すべき暗号鍵を決定するなどすればよい。

【００４８】また、暗号鍵管理プログラム３１２は、この暗号鍵の更新を予め定められた期間ごとに行ってもよいが、そのサイクルにも不規則性を持たせれば、さらにセキュリティを高めることが可能である。この不規則性を持たせる方法としては、たとえばパーソナルコンピュータ３のシステム時刻を取得し、この取得したシステム時刻をもとに予め定められた関数演算を実行して各暗号鍵の有効期間を決定するなどすればよい。

【００４９】次に、図５を参照して、この暗号鍵管理プログラム３１２による暗号鍵の更新の第２の動作原理を説明する。

【００５０】いま、暗号鍵リスト３４１には、暗号鍵（１）～（ｎ）の複数の暗号鍵が記されており、また、システムメモリ３２には、当初、暗号鍵（１）～（２）が暗号鍵３２１として設定されているものと想定する。つまり、ここでは、一時に設定可能な数であるたとえば４つのうちの半数の２つの暗号鍵を設定する。

【００５１】ある期間の経過後、暗号鍵管理プログラム３１２は、予め定められた規則に基づき、磁気ディスク装置３４の暗号鍵リスト３４１から暗号鍵（５）～（６）を選択し、これをシステムメモリ３２に新たな暗号鍵３２１として再設定する。

【００５２】これに伴い、無線ＬＡＮ送受信制御プログラム３１１は、データを暗号化する際に用いる暗号鍵の候補を暗号鍵（５）～（６）の２つとする。しかし、無線ＬＡＮ送受信制御プログラム３１１は、この暗号鍵が更新された時から予め定められた期間内に限り、データを復号する際に用いる暗号鍵の候補を暗号鍵（５）～（６）の２つに更新前の暗号鍵（１）～（２）を加えた合計４つとする。

【００５３】さらにある期間の経過後、暗号鍵管理プログラム３１２は、予め定められた規則に基づき、磁気ディスク装置３４の暗号鍵リスト３４１から暗号鍵（１８）～（１９）を選択し、これをシステムメモリ３２に新たな暗号鍵３２１として再設定する。これに伴い、無

線ＬＡＮ送受信制御プログラム３１１は、データを暗号化する際に用いる暗号鍵の候補を暗号鍵（１８）～（１９）の２つとし、この暗号鍵が更新された時から予め定められた期間内に限り、データを復号する際に用いる暗号鍵の候補を暗号鍵（１８）～（１９）の２つに更新前の暗号鍵（５）～（６）を加えた合計４つとする。

【００５４】同様に、さらにある期間の経過後、暗号鍵管理プログラム３１２は、予め定められた規則に基づき、磁気ディスク装置３４の暗号鍵リスト３４１から暗号鍵（３２）～（３３）を選択し、これをシステムメモリ３２に新たな暗号鍵３２１として再設定し、無線ＬＡＮ送受信制御プログラム３１１は、データを暗号化する際に用いる暗号鍵の候補を暗号鍵（３２）～（３３）の２つとするとともに、この暗号鍵が更新された時から予め定められた期間内に限り、データを復号する際に用いる暗号鍵の候補を暗号鍵（３２）～（３３）の２つに更新前の暗号鍵（１８）～（１９）を加えた合計４つとする。

【００５５】つまり、暗号鍵管理プログラム３１２は、暗号鍵の更新を更新前と更新後とで重複することなく実行するが、無線ＬＡＮ送受信制御プログラム３１１が、更新前の暗号鍵を予め定められた期間内に限り許容することにより、複数の装置間での暗号鍵の更新タイミングのずれを適切な範囲内で吸収する。そして、このために、暗号鍵管理プログラム３１２は、暗号鍵の設定数を一時に取り扱い可能な数の半数以下とする。

【００５６】このように、この暗号鍵更新システムでは、たとえば１年分の暗号鍵をすべての装置に予め配布しておき、各装置が、これらの中から暗号化および復号に用いる暗号鍵を他の装置と同じ規則で選択するようにしたことにより、ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることなく、データを送受信するすべての装置の暗号鍵を同期的に更新することを可能とする。

【００５７】次に、図６および図７を参照して、この暗号鍵更新システムの動作手順を説明する。

【００５８】図６は、暗号鍵管理プログラム３１２の動作手順を説明するためのフローチャートである。

【００５９】暗号鍵管理プログラム３１２は、まず、このパーソナルコンピュータ３のシステム時刻を取得する（ステップＡ１）。システム時刻を取得すると、暗号鍵管理プログラム３１２は、その取得したシステム時刻をもとに暗号鍵選択用に予め与えられた関数演算を実行し、磁気ディスク装置３４に格納された暗号鍵リスト３４１の中から新たな暗号鍵を選択する（ステップＡ２）。

【００６０】新たな暗号鍵を選択すると、暗号鍵管理プログラム３１２は、その選択した暗号鍵をシステムメモリ３２に暗号鍵３２１として設定する（ステップＡ３）。そして、暗号鍵管理プログラム３１２は、先に取得したシステム時刻をもとに有効期間算出用に予め与えられた関数演算を実行し、この新たな暗号鍵の有効期間を算出する（ステップＡ４）。

【００６１】最後に、暗号鍵管理プログラム３１２は、その算出した有効期間後に自身を再起動するための起動タイマを設定し（ステップＡ５）、この処理を終了する。

【００６２】図７は、無線ＬＡＮ送受信制御プログラム３１１の復号時における動作手順を説明するためのフローチャートである。

【００６３】無線ＬＡＮ送受信制御プログラム３１１は、無線信号送受信装置３５を介してアクセスポイント２からのデータを受信すると、システムメモリ３２に設定された暗号鍵の中のパケットで指定された番号の暗号鍵を用いてこのデータの復号を試みる（ステップＢ１）。

【００６４】この復号が成功すると（ステップＢ２のＹＥＳ）、無線ＬＡＮ送受信制御プログラム３１１による復号処理は終了であるが、一方、失敗すると（ステップＢ２のＮＯ）、無線ＬＡＮ送受信制御プログラム３１１は、システムメモリ３２に設定された暗号鍵３２１の更新から予め定められた期間内かどうかを調べる（ステップＢ３）。

【００６５】予め定められた期間内であれば（ステップＢ３のＹＥＳ）、無線ＬＡＮ送受信制御プログラム３１１は、今度は、更新前の旧暗号鍵の中のパケットで指定された番号の旧暗号鍵を用いてこのデータの復号を試みる（ステップＢ４）。

【００６６】そして、復号が成功すれば（ステップＢ７のＹＥＳ）、無線ＬＡＮ送受信制御プログラム３１１による復号処理は終了となり、一方、失敗するか（ステップＢ５のＮＯ）、あるいは、暗号鍵３２１の更新から予め定められた期間内でなかったとき（ステップＢ３のＮＯ）、無線ＬＡＮ送受信制御プログラム３１１は、アクセスポイント２にエラー返答を通知する（ステップＢ６）。

【００６７】なお、この図７で示した無線ＬＡＮ送受信制御プログラム３１１の復号時における動作手順は、暗号鍵管理プログラム３１２が図５に示した第２の動作原理で暗号鍵を更新する場合のものであり、暗号鍵管理プログラム３１２が図４に示した第１の動作原理で暗号鍵を更新する場合には、ステップＢ２における復号が失敗した時点で、ステップＢ６のエラー返答の通知を行えばよい。

【００６８】ところで、この暗号鍵リスト３４１を配布してシステムを起動させた後は、この暗号鍵リスト３４１自体を暗号化して授受することができるようになる。したがって、これ以降は、頒布用のフロッピィディスクに暗号鍵リスト３４１を格納して配布し、各装置側でフロッピィディスク装置３３により読み出して設定するな

どといったことを一切不要とすることが可能となる。そして、そのために、この暗号鍵更新システムでは、アップデートプログラム３１３を準備する。

【００６９】ネットワーク管理サーバコンピュータ１から送信される暗号鍵リストが無線信号送受信部装置３５により受信されると、まず、無線ＬＡＮ送受信制御プログラム３１１が、アクセスポイント２によって暗号化された暗号鍵リストの復号を実行する。そして、この復号された暗号鍵リストは、アップデートプログラム３１３に転送され、アップデートプログラム３１３によって、磁気ディスク装置３４の暗号鍵リスト３４１の更新が実行される。

【００７０】また、セキュリティをより高めるために、このアップデートプログラム３１３に、暗号鍵管理プログラム３１２の更新機能をもたせることも有効である。つまり、ネットワーク管理サーバコンピュータ１から暗号化された新たな暗号鍵管理プログラムを送信し、この暗号化された新たな暗号鍵管理プログラムを無線ＬＡＮ送受信制御プログラム３１１に復号させた後、アップデートプログラム３１３に暗号鍵管理プログラム３１２の更新を実行させる。これにより、暗号鍵の選択規則も人手を介さずに更新できることになり、かつ、暗号が破られる危険性を低くすることが可能となる。

【００７１】

【発明の効果】以上、詳述したように、この発明によれば、たとえば１年分の暗号鍵をすべての装置に予め配布しておき、各装置が、これらの中から暗号化および復号に用いる暗号鍵を他の装置と同じ規則で選択するようにしたため、その結果として、すべての装置が同期を取って暗号鍵を自動的に更新することが可能となり、ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることがない。

【００７２】また、暗号鍵の更新サイクルに不規則性を持たせることにより、セキュリティをより向上させることが可能となる。

【００７３】さらに、たとえば更新前と更新後とで暗号鍵を少なくとも１つは重複させ、あるいは、予め定められた期間内に限り更新前の暗号鍵を復号用の暗号鍵の候補に加えることにより、暗号鍵の更新時にもデータの送受信を中断させることを防止し、あるいは、複数の装置間での暗号鍵の更新タイミングのずれを適切な範囲内で吸収することを可能とする。

【図面の簡単な説明】

【図１】この発明の実施形態に係る暗号鍵更新システムが適用される通信システムのネットワーク構成図。

【図２】同実施形態の暗号鍵更新システムで実行される暗号鍵の更新の概要を示すための概念図。

【図３】同実施形態の通信システムを構成する各装置に備えられる暗号鍵更新システムに関わる構成を示すブロック図。

【図４】同実施形態の暗号鍵管理プログラムによる暗号鍵の更新の第１の動作原理を説明するための図。

【図５】同実施形態の暗号鍵管理プログラムによる暗号鍵の更新の第２の動作原理を説明するための図。

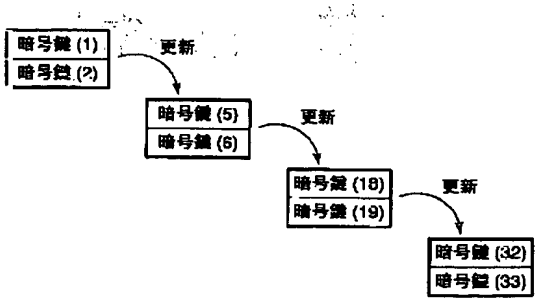
【図６】同実施形態の暗号鍵管理プログラムの動作手順を説明するためのフローチャート。

【図７】同実施形態の無線ＬＡＮ送受信制御プログラムの復号時における動作手順を説明するためのフローチャート。

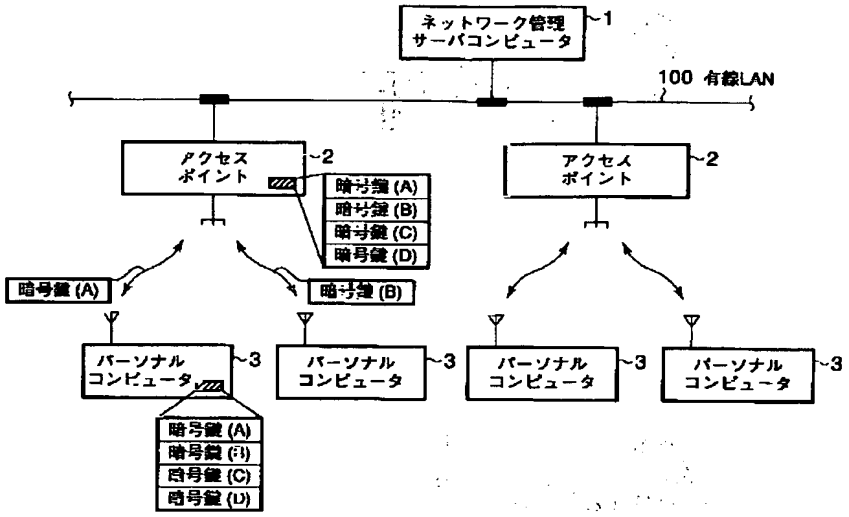
【符号の説明】

１…ネットワーク管理サーバコンピュータ
２…アクセスポイント
３…パーソナルコンピュータ
３１…ＣＰＵ
３２…システムメモリ
３３…フロッピィディスク
３４…磁気ディスク装置
３５…無線信号送受信装置
１００…有線ＬＡＮ
３１１…無線ＬＡＮ送受信制御プログラム
３１２…暗号鍵管理プログラム
３１３…アップデートプログラム
３２１…暗号鍵
３４１…暗号鍵リスト

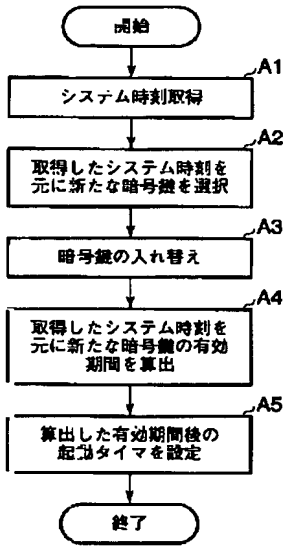
【図５】



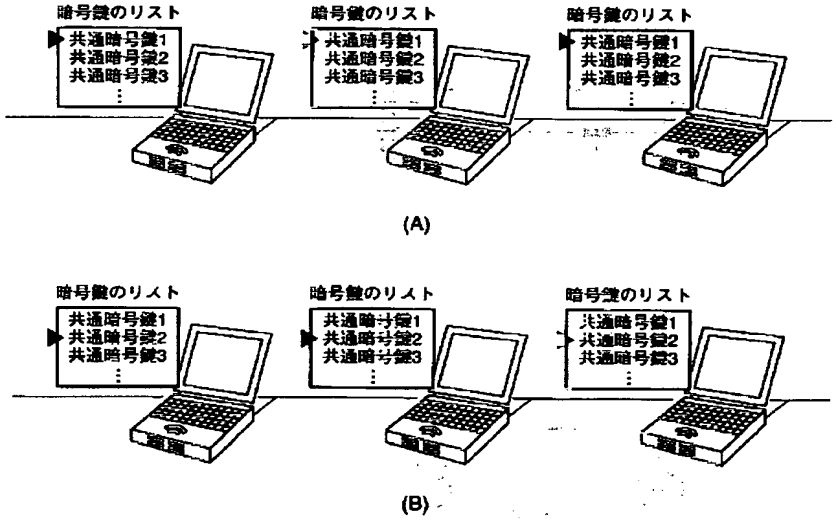
【図1】


ネットワーク管理
サーバコンピュータ
1
100 有線LAN
アクセス
ポイント
2
暗号鍵 (A)
暗号鍵 (B)
暗号鍵 (C)
暗号鍵 (D)
アクセス
ポイント
2
暗号鍵 (A)
暗号鍵 (B)
パーソナル
コンピュータ
3
パーソナル
コンピュータ
3
パーソナル
コンピュータ
3
パーソナル
コンピュータ
3
暗号鍵 (A)
暗号鍵 (B)
暗号鍵 (C)
暗号鍵 (D)

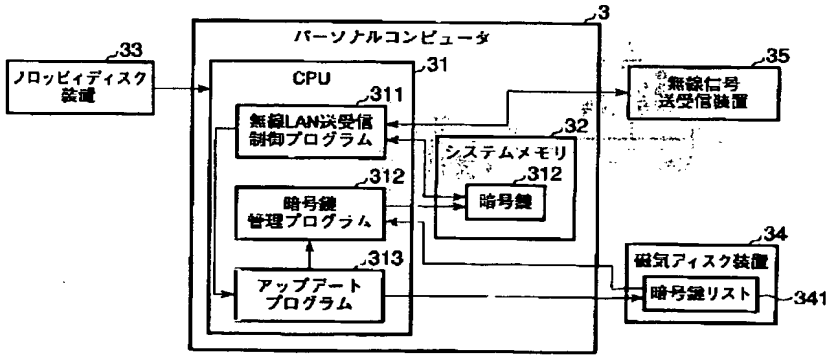
【図6】


開始
A1
システム時刻取得
A2
取得したシステム時刻を
元に新たな暗号鍵を選択
A3
暗号鍵の入れ替え
A4
取得したシステム時刻を
元に新たな暗号鍵の有効
期間を算出
A5
算出した有効期間後の
起動タイマを設定
終了

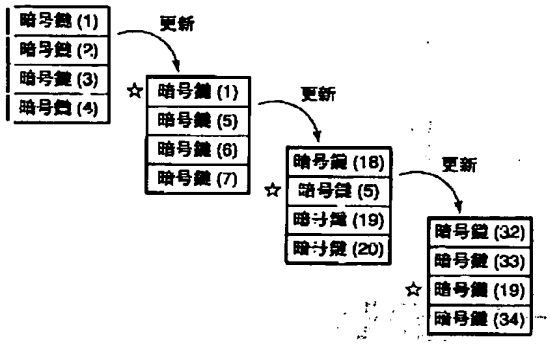
【図2】


暗号鍵のリスト
共通暗号鍵1
共通暗号鍵2
共通暗号鍵3
暗号鍵のリスト
共通暗号鍵1
共通暗号鍵2
共通暗号鍵3
暗号鍵のリスト
共通暗号鍵1
共通暗号鍵2
共通暗号鍵3
(A)
暗号鍵のリスト
共通暗号鍵1
共通暗号鍵2
共通暗号鍵3
暗号鍵のリスト
共通暗号鍵1
共通暗号鍵2
共通暗号鍵3
暗号鍵のリスト
共通暗号鍵1
共通暗号鍵2
共通暗号鍵3
(B)

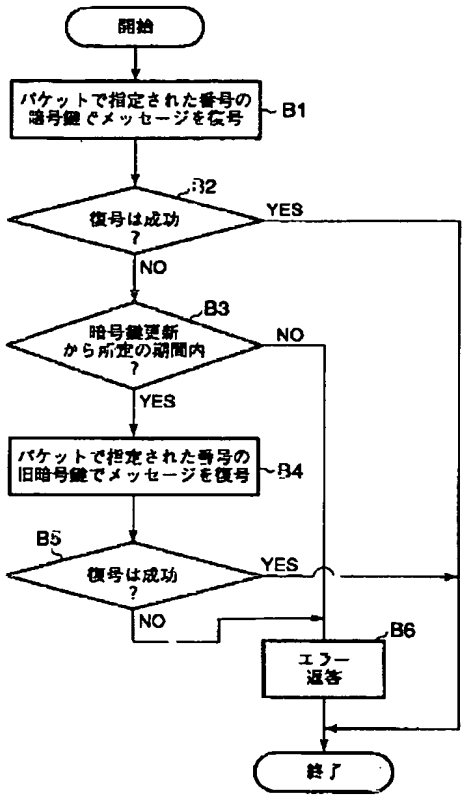
【図3】


3
パーソナルコンピュータ
33
フロッピィディスク
装置
CPU
31
311
無線LAN送受信
制御プログラム
312
暗号鍵
管理プログラム
313
アップデート
プログラム
32
システムメモリ
312
暗号鍵
35
無線信号
送受信装置
34
磁気ディスク装置
暗号鍵リスト
341

【図4】


暗号鍵 (1)
暗号鍵 (2)
暗号鍵 (3)
暗号鍵 (4)
更新
暗号鍵 (1)
暗号鍵 (5)
暗号鍵 (6)
暗号鍵 (7)
更新
暗号鍵 (18)
暗号鍵 (5)
暗号鍵 (19)
暗号鍵 (20)
更新
暗号鍵 (32)
暗号鍵 (33)
暗号鍵 (19)
暗号鍵 (34)

【図7】


開始
パケットで指定された番号の暗号鍵でメッセージを復号
B1
復号は成功？
B2
YES
NO
暗号鍵更新から所定の期間内？
B3
NO
YES
パケットで指定された番号の旧暗号鍵でメッセージを復号
B4
復号は成功？
B5
YES
NO
エラー返答
B6
終了